サイバーセキュリティ対策通信

大阪府警察本部サイバーセキュリティ対策課

アカウント・パスワード管理の甘さが命取り！

不適切なアカウント管理・認証設定が
不正アクセスの原因となることがあります！



大量の個人情報の漏洩事案が相次いでいます。
インターネットに公開されているシステムは特に攻撃の対象となりやすいため
「いつ攻撃を受けてもおかしくない」という前提で対策を講じることが重要です。
適切な認証対策により、不正アクセスのリスクを大幅に低減させることが可能です。

「アカウント管理・認証」の基本対策

対策1 多要素認証（MFA）を導入する

・「知識情報」であるパスワードだけではなく、スマートフォンに届いたSMSを介した番号入力などの「所有情報」や指紋認証などの「生体情報」等も加えた多要素認証を利用してください。
・ID・パスワード流出時の乗っ取りを困難にできるので、安全性が向上します。

対策2 パスワードを強化する

・初期設定のままにしない。
・推測されにくいパスワードを設定する。
・パスワードを使い回さない。

～ 悪いパスワードの例 ～
・連続した数字（123456）
・単純な単語やその類似系（Password、p@ssw0rd）
・名前や生年月日（taro1203）
・キーボードの配列（qwerty,1qaz2wsx）

対策3 管理者アカウントの利用者、アクセス権を最小限にする

・むやみにアカウントを作成せず、作成したアカウントに過剰な管理者権限や更新権限を与えない。
・管理者権限の運用作業手順や作業記録方法等を整理する。

対策4 退職者などの利用されていない不要なアカウントの無効化

・退職者のIDを無効化していないと、情報窃取や不正操作をされる恐れがあります。

～企業のみなさまへ～

サイバー攻撃による被害は、もはや情報システム部門だけの問題ではありません。
サイバーセキュリティ対策を経営課題と位置づけ、必要な投資や人的体制整備を含む対策の強化をお願いします。



その他サイバー犯罪対策に関する事は
大阪府警察のウェブサイトやXを確認ください

大阪府警察ウェブサイト

大阪府警察サイバーセキュリティ対策情報 X